

# Отчёт по лабораторной работе №5

дисциплина: Информационная безопасность

Зорин Илья Михайлович

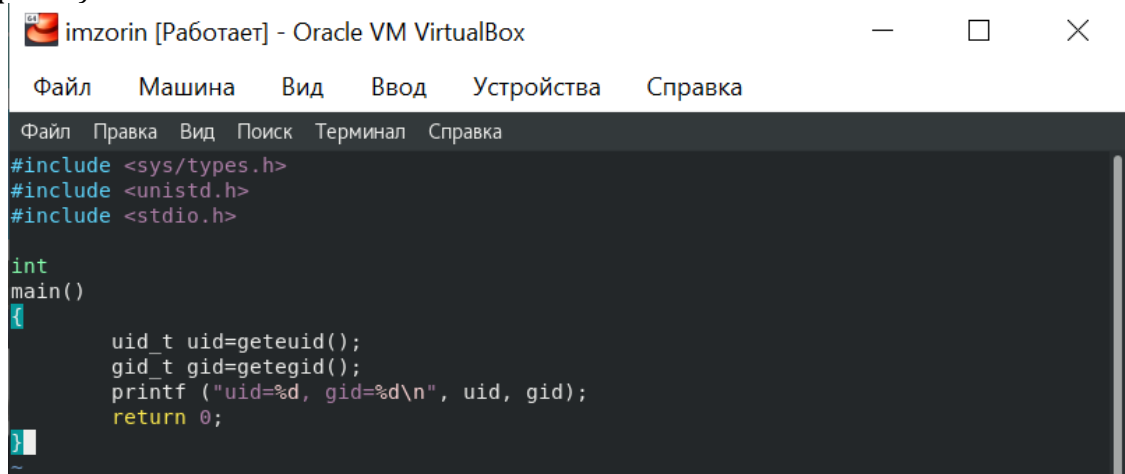
## Содержание

### Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

### Выполнение лабораторной работы

1. Вошёл в систему от имени пользователя guest и создал программу simpleid.c (рис. 1).

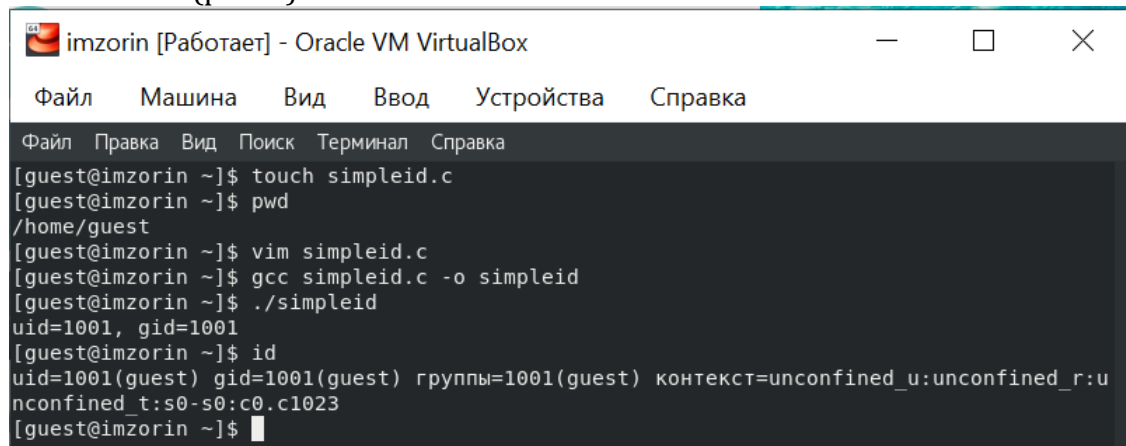


```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Справка
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t uid=geteuid();
    gid_t gid=getegid();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

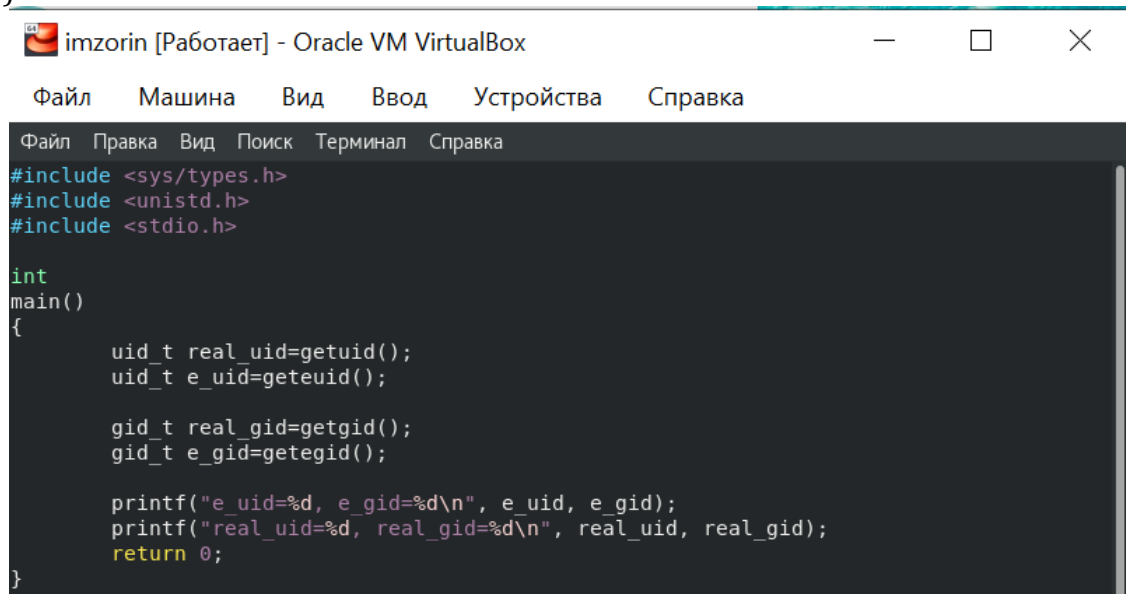
2. Скомпилировал программу и убедился, что файл программы создан. Выполнил программу simpleid. Выполнил системную программу id. В отличие от команды id, моя программа не выводит контекст и все группы, в которые

пользователь (рис. 2).



```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@imzorin ~]$ touch simpleid.c
[guest@imzorin ~]$ pwd
/home/guest
[guest@imzorin ~]$ vim simpleid.c
[guest@imzorin ~]$ gcc simpleid.c -o simpleid
[guest@imzorin ~]$ ./simpleid
uid=1001, gid=1001
[guest@imzorin ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@imzorin ~]$
```

- Усложнил программу, добавив вывод действительных идентификаторов (рис. 3).



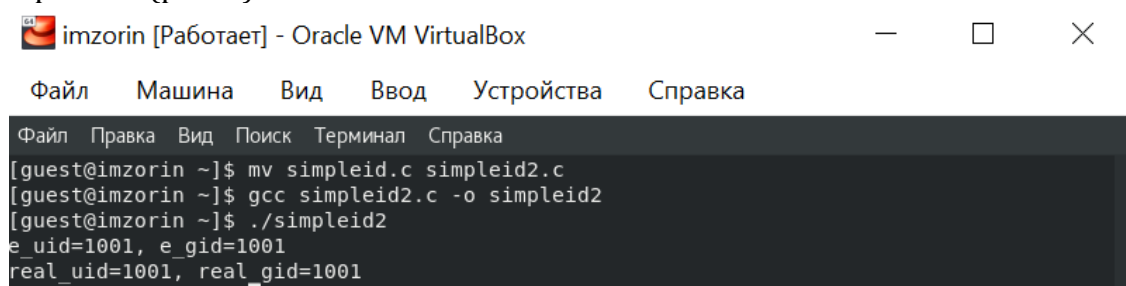
```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Справка
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t real_uid=getuid();
    uid_t e_uid=geteuid();

    gid_t real_gid=getgid();
    gid_t e_gid=getegid();

    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
    return 0;
}
```

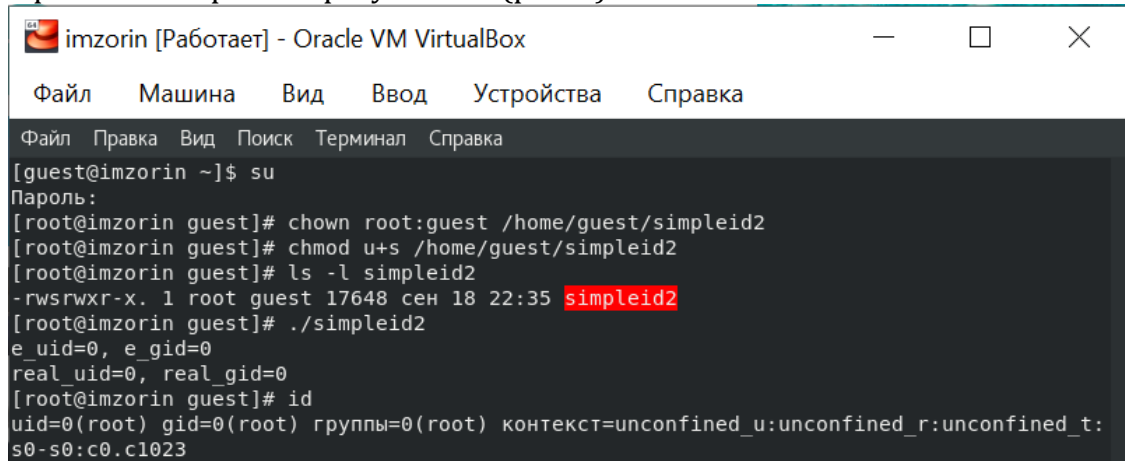
- Получившуюся программу назвал simpleid2.c. Скомпилировал и запустил simpleid2.c (рис. 4).



```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@imzorin ~]$ mv simpleid.c simpleid2.c
[guest@imzorin ~]$ gcc simpleid2.c -o simpleid2
[guest@imzorin ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
```

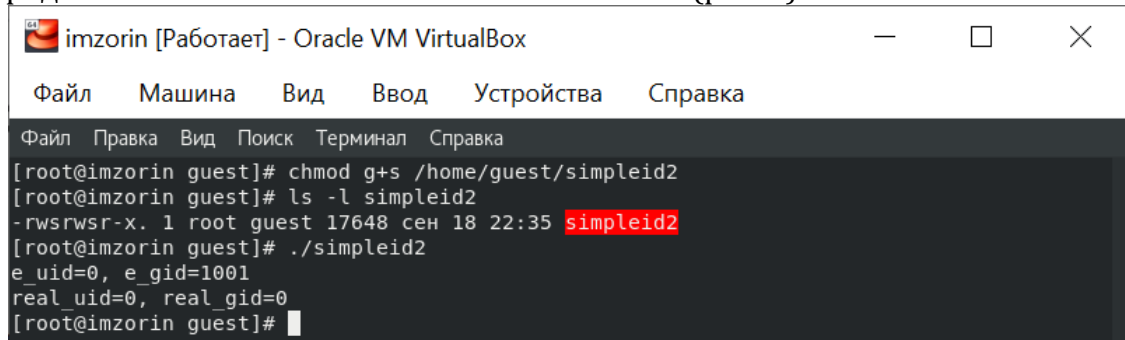
- От имени суперпользователя выполнил команды `chown root:guest /home/guest/simpleid2` и `chmod u+s /home/guest/simpleid2`. Первая команда меняет владельца файла simpleid2 на группу guest. Вторая команда меняет

права доступа к файлу simpleid2 для пользователя и установленные атрибуты SUID или SGID позволяют запускать файл на выполнение с правами владельца файла или группы соответственно. Выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустил simpleid2 и id. Сравнил результаты (рис. 5).



```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@imzorin ~]$ su
Пароль:
[root@imzorin guest]# chown root:guest /home/guest/simpleid2
[root@imzorin guest]# chmod u+s /home/guest/simpleid2
[root@imzorin guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 17648 сен 18 22:35 simpleid2
[root@imzorin guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@imzorin guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

6. Проделал тоже самое относительно SetGID-бита (рис. 6).



```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@imzorin guest]# chmod g+s /home/guest/simpleid2
[root@imzorin guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 17648 сен 18 22:35 simpleid2
[root@imzorin guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@imzorin guest]#
```

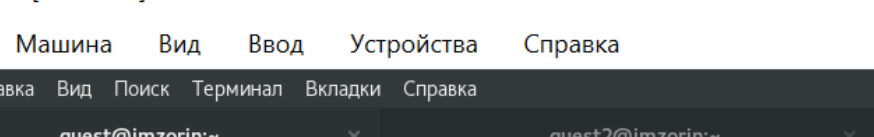
7. Создал программу readfile.c (рис. 7).

8. Откомпилировал программу. Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог. Проверил, что пользователь guest не может прочитать файл readfile.c. Сменил у программы readfile владельца и установил SetU'D-бит. Проверил,

может ли программа readfile прочитать файл readfile.c (рис. 8).

[illegible]

9. Выяснил, установлен ли атрибут Sticky на директории /tmp. От имени пользователя guest создал файл file01.txt в директории/tmp со словом test. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные» (рис. 9).



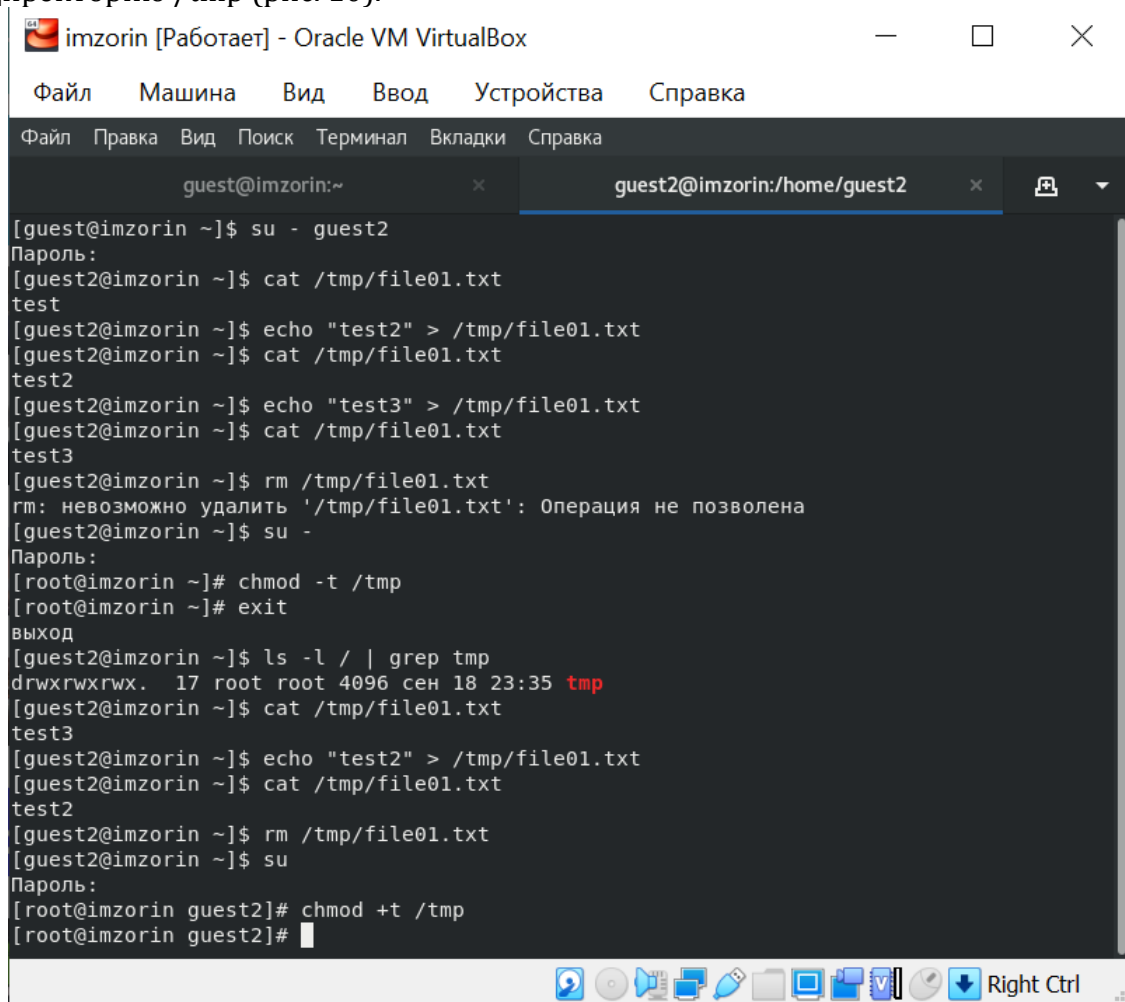
imzorin [Работаer] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Файл Правка Вид Поиск Терминал Вкладки Справка

```
guest@imzorin:~  
[guest@imzorin ~]$ ls -l / | grep tmp  
drwxrwxrwt. 17 root root 4096 сен 18 23:26 tmp  
[guest@imzorin ~]$ echo "test" > /tmp/file01.txt  
[guest@imzorin ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 сен 18 23:31 /tmp/file01.txt  
[guest@imzorin ~]$ chmod o+rw /tmp/file01.txt  
chmod: невозможно получить доступ к '/tmp/file01.txt': Нет такого файла или каталога  
[guest@imzorin ~]$ chmod o+rw /tmp/file01.txt  
[guest@imzorin ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 сен 18 23:31 /tmp/file01.txt
```

10. От пользователя guest2 попробовал прочитать файл /tmp/file01.txt. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2. Удалось выполнить операцию. Проверил содержимое файла. От пользователя guest2 попробовал записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию. Удалось выполнить операцию. Проверил содержимое файла. От пользователя guest2 попробовал удалить файл /tmp/file01.tx. Не удалось выполнить операцию. Повысил свои права до суперпользователя и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. Покинул режим суперпользователя. От пользователя guest2 проверил, что атрибута t у директории /tmp нет. Повторил предыдущие шаги. Удалось успешно выполнить каждый шаг. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp (рис. 10).



```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка
guest@imzorin:~
[guest@imzorin ~]$ su - guest2
Пароль:
[guest2@imzorin ~]$ cat /tmp/file01.txt
test
[guest2@imzorin ~]$ echo "test2" > /tmp/file01.txt
[guest2@imzorin ~]$ cat /tmp/file01.txt
test2
[guest2@imzorin ~]$ echo "test3" > /tmp/file01.txt
[guest2@imzorin ~]$ cat /tmp/file01.txt
test3
[guest2@imzorin ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@imzorin ~]$ su -
Пароль:
[root@imzorin ~]# chmod -t /tmp
[root@imzorin ~]# exit
выход
[guest2@imzorin ~]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 сен 18 23:35 tmp
[guest2@imzorin ~]$ cat /tmp/file01.txt
test3
[guest2@imzorin ~]$ echo "test2" > /tmp/file01.txt
[guest2@imzorin ~]$ cat /tmp/file01.txt
test2
[guest2@imzorin ~]$ rm /tmp/file01.txt
[guest2@imzorin ~]$ su
Пароль:
[root@imzorin guest2]# chmod +t /tmp
[root@imzorin guest2]#
```

## Выводы

Изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами.

Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.